REMARKS

The present application was filed on September 15, 2005, with claims 1-40. The present application claims priority to PCT application US04/21846, filed July 9, 2004, and U.S. provisional application Serial No. 60/486,127, filed July 10, 2003. Claims 1-40 remain pending in the present application.

Claims 1, 2, 5, 6, 13, 19 and 35-40 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,298,851 (hereinafter "Hendricks").

Claims 3, 4, 7-12, 14-18 and 20-34 are each rejected under 35 U.S.C. §103(a) over Hendricks in view of one or more other cited references.

In this response, Applicants traverse the §103(a) rejections, and amend independent claims 1 and 35-40.

With regard to the §103(a) rejection over Hendricks, the Examiner argues that each and every limitation in claims 1, 2, 5, 6, 13, 19 and 35-40 is taught or suggested by Hendricks. Applicants respectfully disagree.

Independent claim 1 is directed to a method for secure generation of a seed for use in performing one or more cryptographic operations. The method includes the steps of a seed generation server providing a first string to a seed generation client, the seed generation client generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the seed generation server, the seed generation client generating the seed as a function of at least the first string and the second string, and the seed generation server decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string.

An important advantage of the claimed arrangement is that it overcomes the problems associated with conventional seed generation techniques that may result in the seed becoming accessible in plaintext form to entities other than an authentication token and an authentication entity. See the specification at, for example, page 2, lines 1-14, page 3, lines 10-13, and page 6, lines 5-7.

The Examiner in formulating the §103(a) rejection of claim 1 argues that the limitations of claim 1 are met by the teachings in column 42, lines 1-15, of Hendricks, relating to a key agreement protocol. See the Office Action at page 2, last paragraph. Applicants respectfully disagree. This portion of Hendricks provides as follows:

> In a different embodiment, depicted in FIG. 24b, the publisher 282 serves as the sender 4998 and operations center 250 serves as the recipient 4999. Initial key negotiation information 5200 is exchanged between a seed key generation algorithm 5201 at the publisher 282 and a seed key generation algorithm 5202 at the operations center 250. As a result, the seed key generation algorithm 5201 at the publisher 282 and the seed key generation algorithm 5202 at the operations center 250 each generate seed key SK 5203 using, for example, the Elliptic Curve Diffie-Hellman key exchange algorithm, as described in U.S. Pat. No. 4,200,700. The seed key SK 5203 is then used by key sequence generator 5204 at the publisher 282 to generate the first in a sequence of keys, transaction symmetric key SKTi 5206.

The relied-upon portion of Hendricks simply indicates that the sender 4998 and recipient 4999 in FIG. 24b generate a shared key 5203 using the conventional Diffie-Hellman key exchange algorithm. However, the Diffie-Hellman key exchange algorithm does not operate in the manner recited in claim 1. In other words, the Diffie-Hellman key exchange algorithm does not involve a first entity providing a first string to a second entity, the second entity generating a second string, encrypting the second string utilizing a key, and sending the encrypted second string to the first entity, the second entity generating the seed as a function of at least the first string and the second string, and the first entity decrypting the encrypted second string and independently generating the seed as a function of at least the first string and the second string. To the contrary, the Diffie-Hellman key exchange algorithm is summarized in column 2, lines 35-52, of U.S. Patent No. 4,200,770 as follows:

> In the present invention a first converser transforms, in a manner infeasible to invert, a first signal while a second converser transforms, also in a manner infeasible to invert, a second signal. The first converser transmits the transformed first signal to the second converser, keeping the first signal secret, and the second converser transmits the transformed second signal to the first converser, keeping the second signal secret. The first converser then transforms the first signal with the transformed second signal to generate a third signal, representing a secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal. And, the second converser transforms the second signal with the transformed first signal to generate a fourth signal, also representing the secure cipher key, that is infeasible to generate solely by transforming the transformed first signal and the transformed second signal.

The Examiner apparently argues that it would be obvious to modify the Diffie-Hellman algorithm such that the second converser in the passage above would encrypt the transformed

second signal prior to sending it to the first converser, using a key that is also known to the first converser, such that the first converser can decrypt the encrypted transformed second signal and utilize the transformed second signal with the transformed first signal to generate the third signal representing the secure cipher key. See the Office Action at page 3, second paragraph. However, such a modification of the Diffie-Hellman algorithm would be inappropriate for at least two reasons.

First, there is no need to encrypt the transformed second signal as that signal is specifically described in the above passage as being infeasible to invert so as to obtain the original second signal that is kept secret by the second converser. One skilled in the art would therefore not be motivated to modify the Diffie-Hellman algorithm so as to incorporate encryption of the transformed second signal, as it would needlessly complicate the algorithm for no additional benefit. The taking of Official Notice that it would be obvious to encrypt values exchanged in a key exchange protocol is therefore traversed. It is clear that the Diffie-Hellman algorithm is deliberately designed such that the transformed second signal is infeasible to invert so as to obtain the original second signal, and therefore encryption of such a signal would be entirely unnecessary and inappropriate.

Second, the entire purpose of the Diffie-Hellman algorithm is to generate a secure cipher key that is known to both the first and second conversers. If the first and second conversers already had such a key, as would be required to implement the recited encryption and decryption operations alleged to be obvious by the Examiner, there would be no need whatsoever to execute the Diffie-Hellman algorithm at all.

The Examiner argues that the proposed modification of the conventional Diffie-Hellman algorithm would be "to provide secure key generation." However, as is clearly described in the Diffie-Hellman reference, the conventional algorithm in its unmodified form already provides secure key generation without any need to encrypt the first and second transformed signals that are exchanged between the first and second conversers, because both of these transformed signals are infeasible to invert so as to obtain the corresponding secret signals. See column 2, lines 13-22, of U.S. Patent No. 4,200,770. Accordingly, the alleged motivation to modify the Diffie-Hellman algorithm is believed to be a conclusory statement of the type ruled legally insufficient by the both Supreme Court and the Federal Circuit. See *KSR International Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (U.S. 2007), quoting *In re Kahn*,

441 F. 3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.").

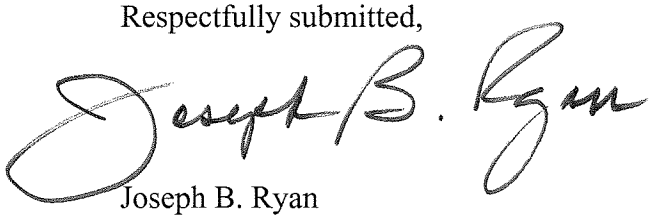
The §103(a) rejection of claim 1 over Hendricks is therefore believed to be improper and should be withdrawn.

Independent claims 35-40 include limitations similar to those of claim 1, and are believed allowable for reasons similar to those outlined above in the context of claim 1.

Dependent claims 2-34 are believed allowable at least by virtue of their dependence from claim 1, and are also believed to define separately-patentable subject matter. The additional references cited by the Examiner fail to supplement the fundamental deficiencies of the Hendricks reference as applied to claim 1.

In view of the foregoing, claims 1-40 are believed to be in condition for allowance.

Respectfully submitted,



Date: June 22, 2009

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517